Android Marcher: Continuously Evolving Mobile Malware

zscaler.de/blogs/research/android-marcher-continuously-evolving-mobile-malware

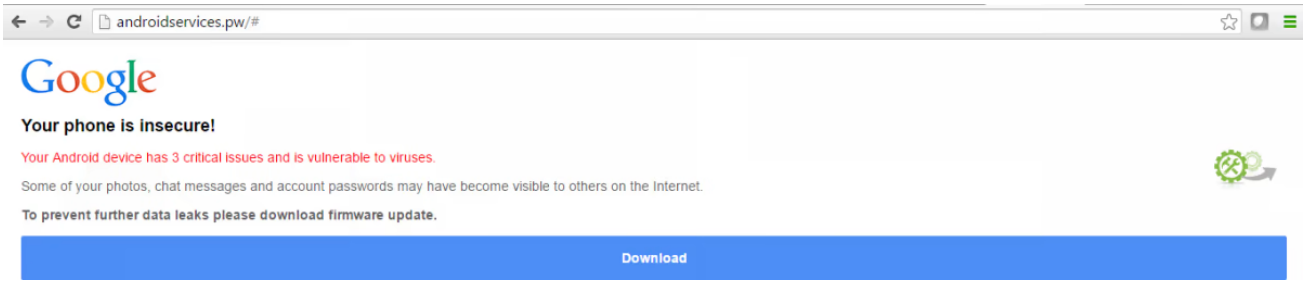
Founded in 2013, the Android Marcher mobile malware has widely been targeting Google Play -- harvesting user credentials and credit card data. The malware waits for victims to open the Google Play store and then displays a fake html overlay page asking for credit card information. The fake page will not go away until the user provides the payment information.

In March 2014, we noticed newer variants targeting financial organizations in Germany. Upon infection, Marcher would inspect the victim's device and send a list of all installed apps to its command and control (C&C) server. If the malware found any German financial apps installed in the device, it would show a fake page asking for credentials of that particular institution. Unaware that the login page is a fake, the victim would provide their credentials where they would then be sent to the malware's C&C. The malware would also show a fake Google Play payment page if the infected device did not have any German financial firm apps. We covered one such sample in a previous blog, see here .

Marcher then started targeting financial firms in Australia, France, Turkey and The United States. Some Marcher samples were observed targeting PayPal as well.

Recently, Marcher added United Kingdom to its hit list, as seen by TrendMicro.

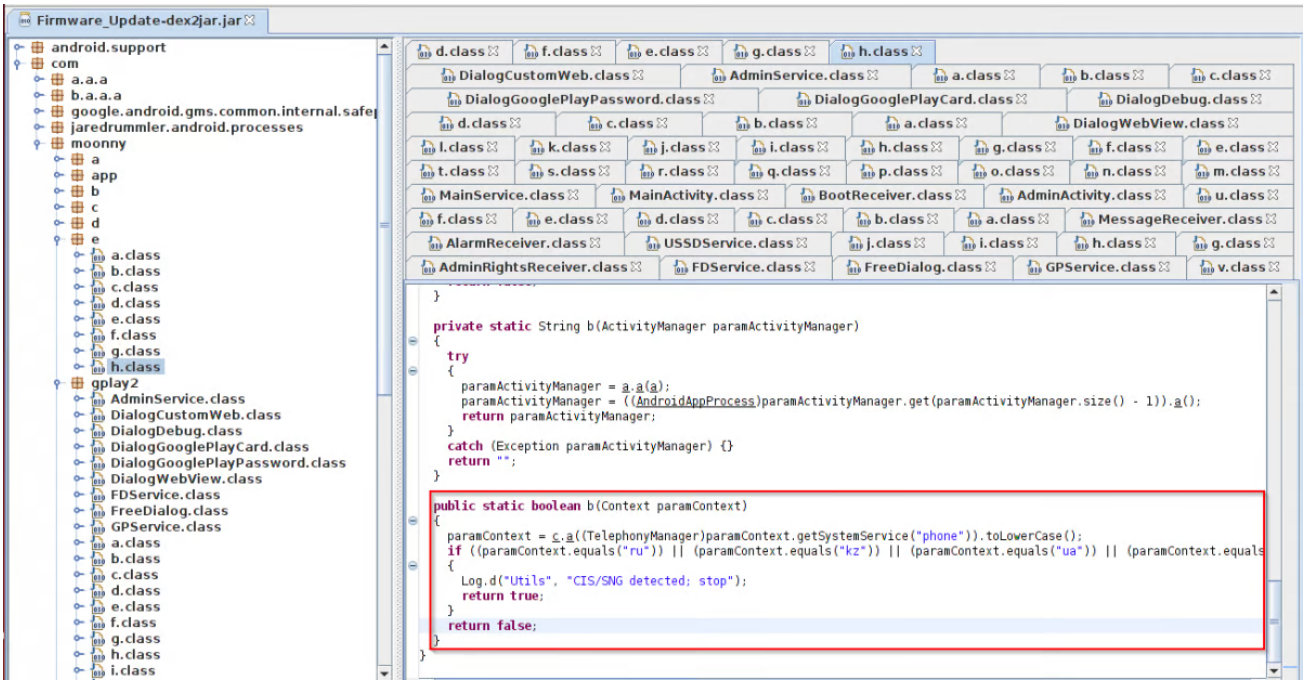
Previously, Marcher was distributed through fake Amazon and Google Play store apps. We've also seen it delivered through a fake porn site that posed as a Chrome update. This month, we observed another new change in the Marcher malware campaign where it is being delivered as a fake Android firmware update. We discovered the payload dropped as "Firmware_Update.apk". An HTML page serving this malware scares the victim by showing that the device is vulnerable to viruses and to prevent personal data theft, prompting them to install the fake update.



Fake update page

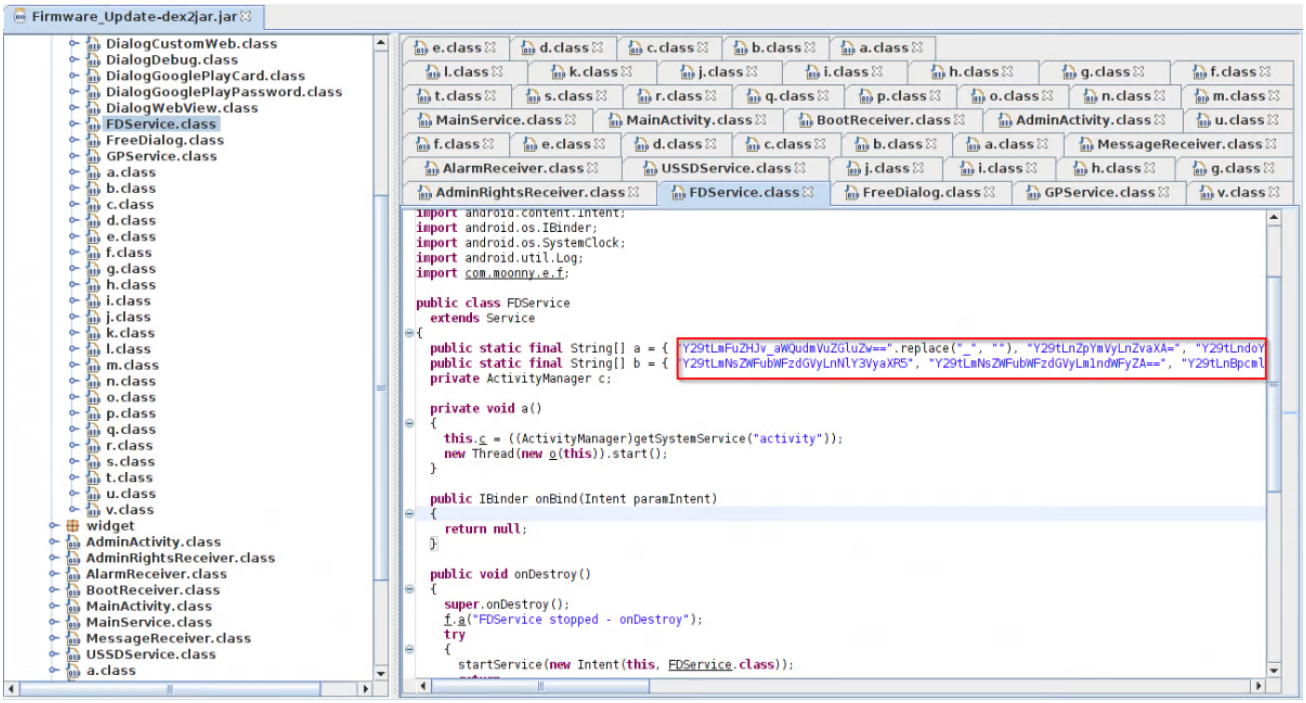
To perform its malicious activity upon installation, Marcher will ask for administrative access.

In 2013, Marcher was only targeting Russian mobile users; however, in the recent samples the author implemented checks to find out if the infected device is from CIS/SIG. It will stop its activity if the device belongs to CIS/SIG territory. Generally, the malware author does this check to avoid any legal cases from its own territory. Such checks indicate that the malware may have been authored and maintained from CIS/SIG countries. See the following screenshot.



CIS/SIG countries check

Another change in this newer variants is implementation of simple obfuscation by the malware author using base64 encoding and string replace functions. In older samples, we did not see this obfuscation. See the following screenshot.

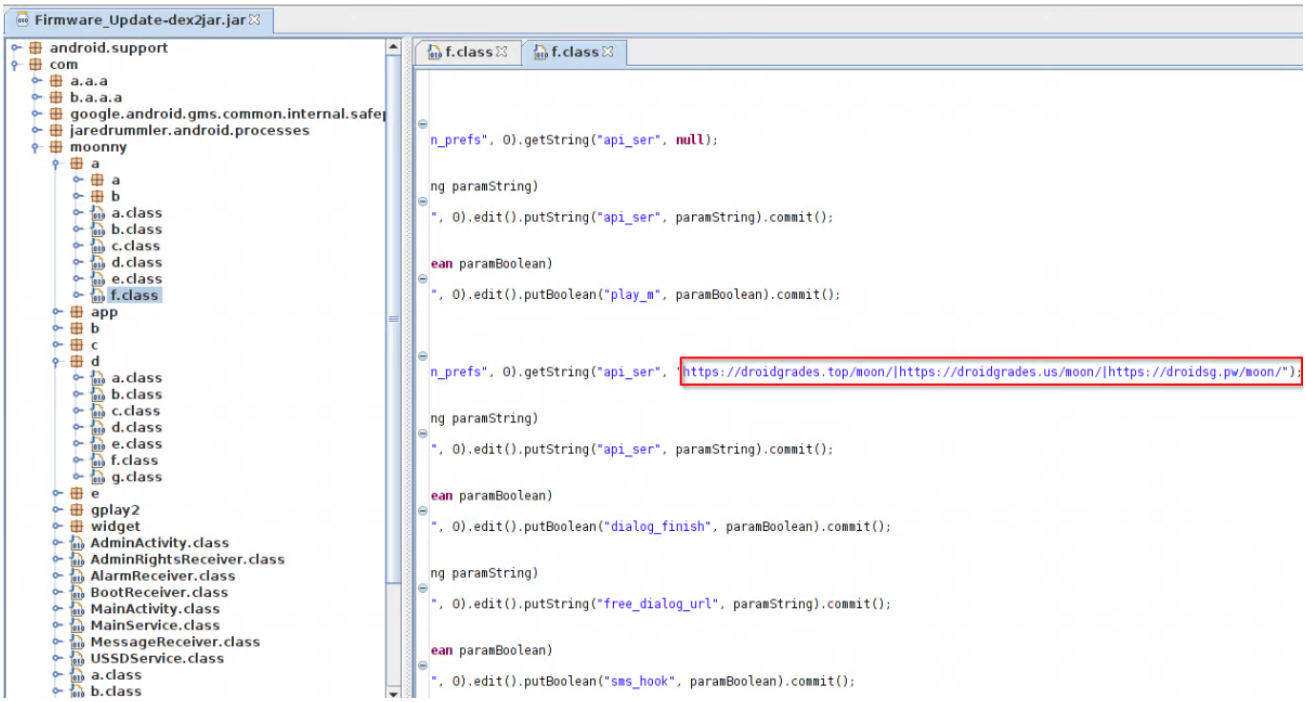


Simple obfuscation techniques

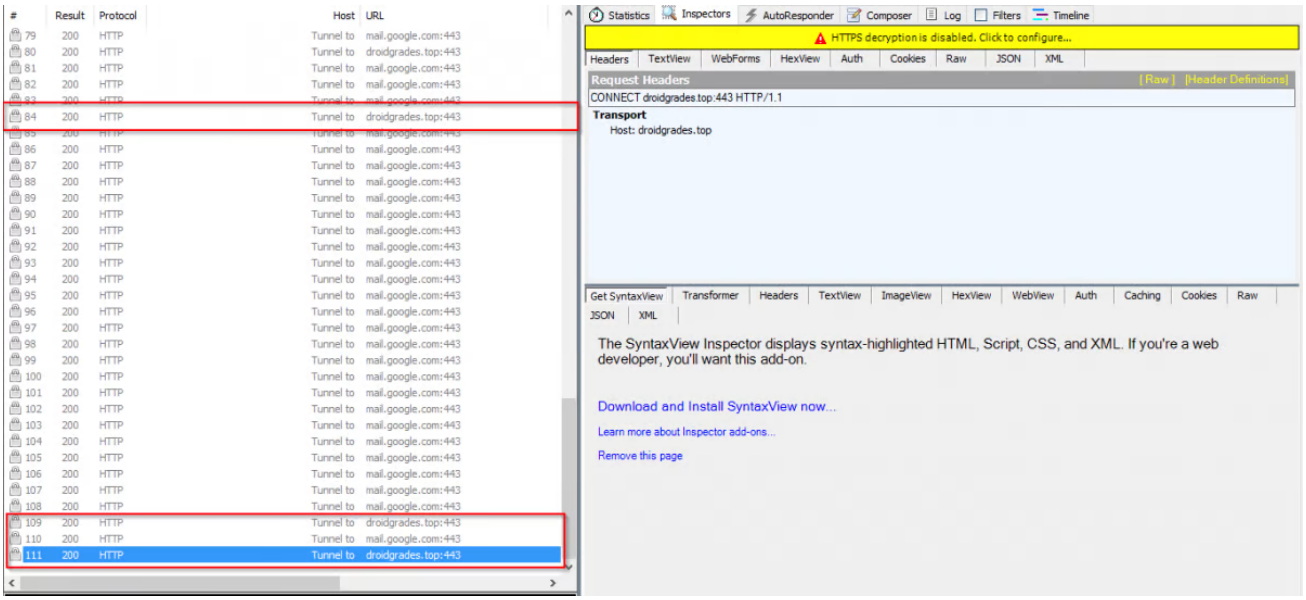
In older Marcher samples we saw that the malware will only show fake a Google Play store credential page if the user opens the Play store app. In recent samples, the malware author implemented checks for multiple well-known apps and shows fake credential page if user opens any of these apps. Following are the apps listed in the code and shown in above screen encoded in base64.

- Playstore (com.android.vending)
- Viber app (com.viber.voip)
- Whatsapp (com.whatsapp)
- Skype (com.skype.raider)
- Facebook messenger (com.facebook.orca)
- Facebook (com.facebook.katana)
- Instagram (com.instagram.android)
- Chrome (com.android.chrome)
- Twitter (com.twitter.android)
- Gmail (com.google.android.gm)
- UC Browser (com.UCMobile.intl)
- Line (jp.naver.line.android)

We have also seen changes related to C&C communication. In older samples the Marcher was communicating on simple http protocol. Now it does C&C communication over SSL. Observe following screen captures.



C&C



C&C over SSL

We are seeing numerous infection attempts in our cloud for this malware family. These frequent changes clearly indicate active malware development that is constantly evolving -- making it the most prevalent threat to the Android devices.

To avoid being a victim of such malware, it is always best to download apps only from trusted app stores, such as Google Play. This can be enforced by unchecking the "Unknown Sources" option under the "Security" settings of your device.

Zscaler ThreatLabZ is actively monitoring this malware and ensuring that Zscaler customers are protected.